

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA

v.

MATTHEW ABIODUN AKANDE,

Defendant

) Criminal No. 22cr10163
)
) Violations:
)
) Count One: Conspiracy to Obtain Unauthorized
) Access to Protected Computers in Furtherance of
) Fraud and to Commit Theft of Government
) Money and Money Laundering
) (18 U.S.C. § 371)
)
) Count Two: Wire Fraud
) (18 U.S.C. § 1343)
)
) Counts Three—Six: Unauthorized Access to
) Protected Computers in Furtherance of Fraud
) (18 U.S.C. § 1030(a)(4))
)
) Counts Seven—Nineteen: Theft of Government
) Money
) (18 U.S.C. §§ 641, 2)
)
) Counts Twenty—Thirty-Three:
) Aggravated Identity Theft
) (18 U.S.C. § 1028A)
)
) Forfeiture Allegation:
) (18 U.S.C. §§ 981(a)(1)(C), 982(a), and
) 28 U.S.C. § 2461)

INDICTMENT

At all times relevant to this Indictment:

General Allegations

1. Defendant MATTHEW ABIODUN AKANDE, a native of Nigeria, resided in Mexico.

2. Coconspirator KEHINDE HUSSEIN OYETUNJI, a native of Nigeria, resided in West Fargo, North Dakota.

3. Coconspirator 1 (“CC-1”) resided in Indonesia.

4. Coconspirator 2 (“CC-2”) and Coconspirator 3 (“CC-3”) resided in or near West Fargo, North Dakota.

5. Victim CPA Firms 1, 2, 3, and 4 were located in Massachusetts and provided tax preparation services for individuals.

6. The Internal Revenue Service (“IRS”) is an agency of the United States within the Department of the Treasury and is responsible for enforcing and administering the United States’ tax laws, including by issuing tax refunds when appropriate.

Overview of the Conspiracy

7. From in or about June 2016 through in or about June 2021, defendant MATTHEW ABIODUN AKANDE conspired with OYETUNJI, CC-1, CC-2, CC-3, and others known and unknown to the Grand Jury to steal money from the U.S. government through the filing of fraudulent tax returns. In addition, beginning no later than in or about February 2020 through in or about February 2021, the conspiracy involved the use of taxpayer information that AKANDE and coconspirators stole from the computer networks of tax preparation firms, including Victim CPA Firms 1, 2, and 4.

Objects and Purpose of the Conspiracy

8. The objects of the conspiracy were:

a. to use fraudulent emails and malicious software to access the computers of

tax preparation firms without authorization to steal confidential—and valuable—client information, including taxpayers’ personally identifiable information (“PII”) and prior years’ tax information;

b. to file with the IRS fraudulent tax returns that claimed tax refunds, including by using taxpayers’ stolen PII and prior years’ tax information; and

c. to commit money laundering by transferring the fraudulently obtained tax refunds in a manner designed to evade detection of the conspiracy.

9. The principal purpose of the conspiracy was to profit by fraudulently obtaining money from the U.S. government.

Manner and Means of the Conspiracy

10. Among the manner and means by which AKANDE, OYETUNJI, CC-1, CC-2, CC-3, and coconspirators known and unknown to the Grand Jury carried out the conspiracy were the following:

a. Preparing remote access trojan malicious software (“RAT malware”) designed to enable remote access to a victim’s computer network;

b. Using specialized encryption software known as a crypter to make the RAT malware undetectable by antivirus software;

c. Tricking tax preparation firms into downloading and executing the RAT malware through fraudulent emails that impersonated prospective clients purporting to seek the tax preparation firms’ services;

d. Using the RAT malware to obtain the PII and prior year tax information of the tax preparation firms' clients;

e. Filing with the IRS fraudulent tax returns that sought tax refunds, including by using taxpayers' PII and prior year tax information stolen from the tax preparation firms;

f. Enlisting coconspirators to open U.S. bank accounts to receive fraudulently obtained tax refunds;

g. Directing U.S. banks to send debit cards associated with the U.S. bank accounts to coconspirators;

h. Directing the IRS to deposit the requested tax refunds into the U.S. bank accounts that the conspiracy controlled;

i. Tracking the filing of fraudulent tax returns, the U.S. bank accounts into which the tax refunds were deposited, and the coconspirators responsible for the U.S. bank accounts;

j. Laundering the fraudulently obtained tax refunds, including by making cash withdrawals from the U.S. bank accounts, transferring the proceeds through money transmitting businesses, and/or converting them to cryptocurrency; and

k. Splitting the fraudulently obtained tax refunds among the coconspirators.

11. In this fashion, between in or about June 2016 and in or about June 2021, AKANDE and his coconspirators filed more than 1,000 fraudulent tax returns, sought over \$8.1 million in fraudulent tax refunds, and successfully obtained over \$1.3 million in fraudulent tax refunds.

Overt Acts in Furtherance of the Conspiracy

12. Between in or about June 2016 and in or about June 2021, AKANDE, OYETUNJI, CC-1, CC-2, CC-3, and coconspirators known and unknown to the Grand Jury committed and caused to be committed the following overt acts, among others, in furtherance of the conspiracy:

RAT Malware Phishing Attacks on Victim CPA Firms

- a. On or about February 15, 2020, AKANDE e-mailed a RAT malware seller that his “target are Certified public accountant [sic] who files individual tax returns” and that “I want to be able to access the client PC to bring out the Tax return PDF info.”
- b. On or about February 16, 2020, AKANDE purchased online a license for RAT malware.
- c. On or about February 19, 2020, AKANDE activated a license for crypter software sold online.
- d. On or about May 27, 2020, AKANDE purchased online a license for RAT malware.
- e. On or about May 27, 2020, AKANDE leased a website domain and created an associated email account that mimicked the name of a Massachusetts-based architectural engineering firm (the “Engineering Firm”).
- f. On or about May 28, 2020, AKANDE sent CC-1 a template email to be sent to victim CPA firms (the “Template Phishing Email”). The Template Phishing Email purported to come from the Chief Executive Officer of the Engineering Firm (the “Victim CEO”). The

Template Phishing Email falsely stated that the Victim CEO was seeking tax preparation services from the CPA firm recipients.

g. That same day, CC-1 sent the Template Phishing Email to Victim CPA Firms 1, 2, 3, and 4 using a technique known as “spoofing,” which caused the emails to appear as if they had been sent by the Victim CEO from the fake domain for the Engineering Firm leased by AKANDE. Without the Victim CEO’s authorization, CC-1 attached to the emails a .pdf file containing the Victim CEO’s genuine 2019 tax reporting materials, including the Victim CEO’s genuine Forms W-2 and 1099.

h. Also on or about May 28, 2020, AKANDE sent the Template Phishing Email to a different CPA firm located in Massachusetts. AKANDE sent the email from the fake domain for the Engineering Firm and made it appear as if it had come from the Victim CEO. AKANDE attached—without the Victim CEO’s authorization—the Victim CEO’s genuine 2019 tax reporting materials, including the Victim CEO’s genuine Forms W-2 and 1099.

i. Between on or about June 1 and on or about June 3, 2020, AKANDE sent more fraudulent emails in the Victim CEO’s name to the owners of Victim CPA Firms 1, 2, 3, and 4. The emails contained a link to a Dropbox account that supposedly contained the Victim CEO’s prior year tax information. In reality, the Dropbox account contained a disguised executable file that, when downloaded and executed, would cause the Victim CPA Firms to unknowingly download RAT malware onto their computer networks. The owners of each of Victim CPA Firms 1, 2, and 3 accessed the link and, as AKANDE intended, unknowingly downloaded RAT malware, which was used to collect each firm’s client PII and prior years’ tax information. The owner of

Victim CPA Firm 4 provided AKANDE (posing as the Victim CEO) a link to their firm's cloud storage location, to which AKANDE uploaded RAT malware, which the owner downloaded and which also thereafter collected Victim CPA Firm 4's client PII and prior years' tax information.

June 30, 2020 Fraudulent Tax Return

j. On or about June 30, 2020, AKANDE caused a fraudulent tax return that sought a refund of \$8,516 to be electronically filed with the IRS in the name of Victim Individual 1, a client of Victim CPA Firm 1 whose PII and prior year tax information AKANDE and his coconspirators collected via the RAT malware. The fraudulent tax return directed the IRS to deposit the requested refund into a Green Dot bank account in the name of Victim Individual 1, which the IRS did on or about July 9, 2020.

k. On or about July 16, 2020, OYETUNJI messaged AKANDE an address in Fargo, North Dakota to which AKANDE should send a debit card to be used to withdraw fraudulent tax refund proceeds.

l. On or about July 16, 2020, AKANDE caused Green Dot to issue a replacement debit card for the account in Victim Individual 1's name and ordered a rush delivery by FedEx to the address that OYETUNJI provided.

m. On or about July 22, 2020, AKANDE messaged OYETUNJI the first name of Victim Individual 1, the word "pin," and a four-digit number.

n. Between on or about July 24 and on or about August 11, 2020, in or around Fargo and West Fargo, North Dakota, OYETUNJI or a coconspirator used the Green Dot debit

card in Victim Individual 1's name to make approximately ten ATM withdrawals and five purchases at retailers (each of which included cash back) totaling more than \$8,400.

o. On or about July 24, 2020—the same day the withdrawals from the Green Dot bank account in Victim Individual 1's name began—AKANDE instructed OYETUNJI to send the conspiracy's proceeds to a person in Mexico ("Mexico Recipient 1").

p. On or about July 27, 2020, OYETUNJI sent the name and location of Mexico Recipient 1 that AKANDE had provided him to CC-2.

q. On or about July 27, 2020, CC-2 sent \$1,390 via Western Union to Mexico Recipient 1.

r. On or about July 29, 2020, AKANDE messaged OYETUNJI the names of two other individuals to whom OYETUNJI should send the conspiracy's proceeds.

s. Later that same day, OYETUNJI messaged AKANDE that CC-3 would be the "sender" and that one of the two individuals ("Mexico Recipient 2") would be the "receiver."

t. Later that same day, CC-3 sent \$1,500 via Western Union to Mexico Recipient 2 at an address in Mexico.

u. Between on or about July 27 and on or about August 14, 2020, CC-2 and CC-3 sent a total of approximately \$7,840 to Mexico Recipients 1 and 2 in Mexico.

Additional Fraudulent Tax Returns

v. Between in or about June 2020 and in or about February 2021, AKANDE caused at least 80 additional fraudulent tax returns seeking tax refunds to be electronically filed

with the IRS in the names of clients of Victim CPA Firms 1, 2, and 4, each of whose PII and prior year tax information AKANDE and coconspirators had stolen via the RAT malware.

[REMAINDER OF PAGE INTENTIONALLY BLANK]

COUNT ONE

Conspiracy to Obtain Unauthorized Access to Protected Computers in Furtherance of Fraud
and to Commit Theft of Government Money and Money Laundering
(18 U.S.C. § 371)

The Grand Jury charges:

13. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 12(v) of this Indictment.

14. From in or about June 2016 through in or about June 2021, in the District of Massachusetts and elsewhere, the defendant,

MATTHEW ABIODUN AKANDE,

conspired with OYETUNJI, CC-1, CC-2, CC-3, and others known and unknown to the Grand Jury to commit offenses against the United States, to wit:

a. unauthorized access to computers, in violation of Title 18, United States Code, Section 1030(a)(4), that is, to knowingly access a protected computer without authorization, with intent to defraud, and by means of such conduct to further the intended fraud and obtain a thing of value, specifically, the personally identifiable information and prior years' tax information of the tax preparation firms' clients;

b. theft of government money, in violation of Title 18, United States Code, Section 641, that is, to knowingly and willfully embezzle, steal, purloin, and convert to his use and the use of another any money and thing of value of the United States and of any department and agency thereof, in a total amount greater than \$1,000, namely, fraudulent tax refunds seeking refunds greater than \$1,000; and

c. money laundering, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i), that is, to conduct and attempt to conduct financial transactions, to wit, cash withdrawals and subsequent wire money transfers, knowing that the property involved in such transactions represented the proceeds of some form of unlawful activity, and which in fact involved the proceeds of specified unlawful activity, that is, theft of government money in violation of Title 18, United States Code, Section 641, and knowing that the transactions were designed, in whole and in part, to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity.

All in violation of Title 18, United States Code, Section 371.

COUNT TWO
Wire Fraud
(18 U.S.C. § 1343)

The Grand Jury further charges:

15. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 12(v) of this Indictment.

16. From in or about February 2020 through in or about February 2021, in the District of Massachusetts and elsewhere, the defendant,

MATTHEW ABIODUN AKANDE,

having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing the scheme to defraud, to wit: an email to a Massachusetts CPA firm on or about May 28, 2020, purporting falsely to be from the Victim CEO and attaching the Victim CEO's genuine 2019 tax reporting materials, including the Victim CEO's genuine Forms W-2 and 1099.

All in violation of Title 18, United States Code, Section 1343.

COUNTS THREE – SIXUnauthorized Access to Protected Computers in Furtherance of Fraud
(18 U.S.C. § 1030(a)(4))

The Grand Jury further charges:

17. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 12(v) of this Indictment.

18. On or about the dates set forth below, in the District of Massachusetts and elsewhere, the defendant,

MATTHEW ABIODUN AKANDE,

knowingly accessed the protected computers below without authorization, with intent to defraud, and by means of such conduct furthered the intended fraud and obtained a thing of value, specifically, the personally identifiable information and prior years' tax information of the tax preparation firms' clients:

Count	Approximate Date	Victim Computer Network
3	June 1, 2020	Victim CPA Firm 2
4	June 2, 2020	Victim CPA Firm 1
5	June 2, 2020	Victim CPA Firm 3
6	June 3, 2020	Victim CPA Firm 4

All in violation of Title 18, United States Code, Section 1030(a)(4).

COUNTS SEVEN – NINETEEN

Theft of Government Money

(18 U.S.C. §§ 641, 2)

The Grand Jury further charges:

19. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 12(v) of this Indictment.

20. On or about the dates set forth below, in the District of Massachusetts and elsewhere, the defendant,

MATTHEW ABIODUN AKANDE,

did knowingly and willfully embezzle, steal, purloin, and convert to his use and the use of another, any money and thing of value of the United States and of any department and agency thereof, in a total amount greater than \$1,000, namely, fraudulent tax refunds in the approximate amounts set forth below:

Count	Approximate Date	Victim Individual	Fraudulent Tax Refund
7	6/5/2020	2	\$4,154
8	6/6/2020	3	\$4,739
9	6/6/2020	4	\$7,008
10	6/9/2020	5	\$4,204
11	6/10/2020	6	\$9,281
12	6/10/2020	7	\$7,215
13	6/29/2020	8	\$4,121
14	6/30/2020	1	\$8,608
15	7/1/2020	9	\$5,027
16	7/1/2020	10	\$5,456
17	2/14/2021	11	\$7,224
18	2/17/2021	12	\$7,853
19	2/19/2021	13	\$14,950

All in violation of Title 18, United States Code, Section 641.

COUNT TWENTY
Aggravated Identity Theft
(18 U.S.C. § 1028A(a)(1))

The Grand Jury further charges:

21. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 12(v) of this Indictment.

22. On or about May 28, 2020, in the District of Massachusetts and elsewhere, the defendant,

MATTHEW ABIODUN AKANDE,

did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, to wit, the name and Social Security number of Victim CEO, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), to wit, wire fraud as charged in Count Two of this Indictment.

All in violation of Title 18, United States Code, Section 1028A(a)(1).

COUNTS TWENTY-ONE – THIRTY-THREEAggravated Identity Theft
(18 U.S.C. § 1028A(a)(1))

The Grand Jury further charges:

23. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 12(v) of this Indictment.

24. On or about the dates set forth below, in the District of Massachusetts and elsewhere, the defendant,

MATTHEW ABIODUN AKANDE,

did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, to wit, the names and Social Security numbers of taxpayers in whose names fraudulent tax returns were filed, during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), to wit, theft of government money, as charged in Counts Seven through Nineteen of this Indictment:

Count	Approximate Date	Victim Individual
21	6/5/2020	2
22	6/6/2020	3
23	6/6/2020	4
24	6/9/2020	5
25	6/10/2020	6
26	6/10/2020	7
27	6/29/2020	8

Count	Approximate Date	Victim Individual
28	6/30/2020	1
29	7/1/2020	9
30	7/1/2020	10
31	2/14/2021	11
32	2/17/2021	12
33	2/19/2021	13

All in violation of Title 18, United States Code, Section 1028A(a)(1).

FORFEITURE ALLEGATION

(18 U.S.C. §§ 981(a)(1)(C), 982(a), and 28 U.S.C. § 2461(c))

25. Upon conviction of one or more of the offenses set forth in Counts One through Nineteen, in violation of Title 18, United States Code, Section 371; Title 18, United States Code, Section 1343; Title 18, United States Code, Section 1030(a)(4); and Title 18, United States Code, Section 641, respectively, the defendant,

MATTHEW ABIODUN AKANDE,

shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 982(a), and Title 28, United States Code, Section 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to the offenses, and, pursuant to Title 18, United States Code, Section 982(a)(1), any property, real or personal, involved in such offenses, and any property traceable to such property.

26. If any of the property described in Paragraph 25, above, as being forfeitable pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 982(a), and Title 28, United States Code, Section 2461(c), as a result of any act or omission of the defendant --

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;

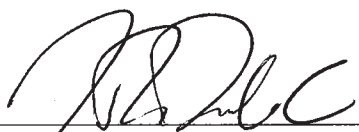
it is the intention of the United States, pursuant to Title 28, United States Code, Section 2461(c)

and Title 18, United States Code, Section 982(b), both incorporating Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendant up to the value of the property described in Paragraph 25 above.

All pursuant to Title 18, United States Code, Sections 982(a)(1)(C) and 982(a), and Title 28, United States Code, Section 2461(c).

A TRUE BILL


FOREPERSON


JAMES R. DRABICK
ASSISTANT UNITED STATES ATTORNEY
DISTRICT OF MASSACHUSETTS

District of Massachusetts: July 19, 2022
Returned into the District Court by the Grand Jurors and filed.


DEPUTY CLERK